PCT/GB 00/ 0 3 6 2 0

GB00/03620

INVESTOR IN PEOPLE

4

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

12/4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

REC'D 18 OCT 2000
WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed M Conkie

Dated 6 October 2000

THE PATENT OFFICE
-4 OCT 1999
RECEIVED BY FAX

Patents Form 1/77

Patents Act 1977
(Rule 16)

The **Patent Office**

04 OCT 99 E481297-1 002806
P01/7700 0.00 - 9923340.5

The Patent Office
Cardiff Road
Newport
Gwent NP9 1RH

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet, from the Patent Office to help you fill in this form)

1. Your reference — JL2255(P2961) — - 4 OCT 1999

2. Patent application number *(The Patent Office will fill in this part)* — **9923340.5**

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

THE SECRETARY OF STATE FOR DEFENCE

DEFENCE EVALUATION AND RESEARCH AGENCY
FARNBOROUGH
HAMPSHIRE
GU14 0LX

Patents ADP number *(if you know it)* 7349996001

If the applicant is a corporate body, give the country/state of its incorporation — UNITED KINGDOM

4. Title of the invention — IMPROVEMENTS RELATING TO SECURITY

5. Name of your agent *(if you have one)* — BARKER BRETTELL

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

138 HAGLEY ROAD
EDGBASTON
BIRMINGHAM
B16 9PW

Patents ADP number *(if you know it)* — 7442494002

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of Filing *(day/month/year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day/month/year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d)) — YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	-
Description	30
Claim(s)	12
Abstract	1
Drawing(s)	4

10. If you are also filing any of the following, state how many against each item.

Priority documents	-
Translations of priority documents	-
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	1
Request for preliminary examination *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	-
Any other documents *(please specify)*	-

11. I/We request the grant of a patent on the basis of this application.

Signature: BARKER BRETTELL — Date: 04.10.99

12. Name and daytime telephone number of person to contact in the United Kingdom: JOHN LAWRENCE — TEL: 0121-456 1364

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 01645 500505
b) Write your answers in capital letters using black ink or you may type them.
c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.
e) Once you have filled in the form you must remember to sign and date it.
f) For details of the fee and ways to pay please contact the Patent Office.

IMPROVEMENTS RELATING TO SECURITY

This invention relates to an improved method of increasing the security of a computer system especially a networked system, together with a computer security apparatus, a secure network, software adapted to provide security, and a software carrier.

It is well known to hold data on a computer system to which it is desired to restrict access. Further, there are various known techniques which can be used to ensure that only people, clients, entitled to access the data can actually do so. However, computer hacking is well known and the computer systems holding such data need to be designed so that the system is as secure as possible, that is there are no security loop holes which can be exploited by potential hackers.

One area where security is important is Internet networked systems. One Internet problem is controlling individual and group access rights to web pages on a web server.

The Internet/web page prior art system is the secure socket layer (SSL) which uses public key cryptographic technology to authenticate clients and then encrypts subsequent communications, allowing clients to access directories and web pages that require presentation of a valid certificate (e.g. their X.509 Certificate).

However, this technique does not provide for varying levels of access: a client can either access the data or they cannot. Further, SSL involves a complex handshake and employs encryption techniques that lead to a major performance degradation. Encryption prevents file compression for

telecommunication transmission. Therefore encrypted files have to be transmitted in uncompressed form, which clearly requires a greater bandwidth, and/or takes longer.

The encryption also prevents content filtering, e.g. at company firewalls, where there is a desire to block browsing of inappropriate material and/or to screen for malicious code, such as computer viruses.

According to a first aspect of the invention there is provided a method of securing data held on a computer network comprising labelling datasets or sections with an access level, determining the access level to which a user or client wishing to access the data is allowed to access and after determining the client's identity allowing the client access only to datasets or sections which have an appropriate access level.

An advantage of such method is that it is simpler to implement and easier to maintain than prior art systems. In prior art systems (such as the SSL system) it has previously been known to note on each data section the identity of clients who are entitled to access that data section and allow only those clients access rights. Therefore, should the rights of a particular client alter (for example a client may leave the employment of a company) it would be necessary to access each dataset or section of a database and alter the reference as necessary for that particular client. Clearly, if there are a large number of data sections this is a time consuming process which is not required in the invention according to the present invention.

The computer network may comprise the Internet. Use of the Internet is convenient because it is a readily available network which is generally

easily accessible. However, the skilled person will appreciate that any network is suitable (any LAN, or WAN may also be suitable).

In particular, the method may make use of the world wide web. In such an implementation the datasets/sections may comprise one or more web page and the access level may determine whether or not the particular web page can be viewed. Such a method is advantageous because allows the datasets/sections to be readily accessed and uses well known technology.

The access levels, or dataset labels, may be provided as tags, such as meta tags, within the HTML code of a particular web page providing a simple and efficient way of noting the access level.

The method may comprise using standard access software provided for the network being used in addition to specific software for providing the method. The standard access software may comprise a web browser and a web server. The skilled person will appreciate that such access software is well known and is readily available. Using such standard software may make the method easier to implement than if specific access components were required.

Conveniently, the specific software for providing the method may communicate with standard access software already provided, providing a simple architecture for the method. In particular, the specific software may provide proxy servers with specific network addresses. To use standard access software to access the data it may be necessary for the standard access software to address the proxy servers, thus providing a convenient way of controlling how the standard access software functions.

A first, user, proxy server may be provided in association with the specific software used to access the data. The first proxy server may run on the same computer as the specific software (which may be a web browser), or may be provided remotely of the computer.

Further, a second, access controller, proxy server may be provided in association with the data. The second proxy server may run on the same computer as the computer storing the data, or perhaps more preferably it may run on a computer remote from the computer holding the data. The data may comprise a collection of web pages managed by a web server. It is preferable that the second proxy server runs remote from the computer holding the data to enhance the security of the system. If the proxy server and the data (possibly a web server) run on the same computer security loop holes in the software managing the data could allow the proxy server to be by-passed, whereas if the proxy server is provided on a separate server/computer the second, access controller, proxy server will only be vulnerable to loop holes in itself. Web servers may be thought of as software managing the data and are generally complex programs and it is thus hard to ensure that they are free of loop holes which may allow people by-pass them.

The method may allow clients without the necessary specific access software to access datasets/sections. Preferably, clients without the specific access software are assigned a predetermined access level which in general may be the lowest access level granting such a client only minimum access to the data.

The method may make use of the challenge response technique to verify the identity of the client wishing to access the data. This is a well known

and tested technique. The client may need to provide an appropriate response to a challenge before each data section is provided to the client.

Conveniently the method initially comprises the client passing a request for data across the computer network. This request for data may then provoke a challenge from the network to which the client must make an appropriate response in order to verify their identity. Once the identity of the client has been confirmed the method may comprise the step of checking whether the client has the necessary access level to receive the data they have requested. Checking of the access level held by the client may be achieved by looking up an entry held on the computer network for that particular client. Once the access level assigned to the client has been determined it may be compared to the access level held on the requested data section. If the client has an appropriate access level then the requested data section may be passed to the client. If the access level assigned is not appropriate then access may be denied.

The identity of the client may be verified using a certificate held by the client. Generally, the certificate is obtained from an independent standards authority and has associated with it a public and a private key which can be used to determine the identity of a client presenting a particular certificate. The skilled person will appreciate that such techniques are well known. In one embodiment an X.509 certificate is used to verify the identity of the client.

The certificate may identify the client to whom it belongs at a number of different levels and each level may be a subset of previous level. Each level may provide a specific level of access to the data. The access level associated with known level may be held on the computer network, and is preferably associated with the second proxy server. Preferably the access

levels are held within a look up table, and once the identity of the client has been verified the access levels can be determined.

Preferably, the method comprises sending data sections across the computer network in an un-encrypted form. This allows the data to be compressed for transmission, with the advantages this brings (e.g. speed of transmission, reduced bandwidth requirement etc.). Transmitting unencrypted data is also advantageous because it allows the content of the data to be screened. Should the method be applied across the Internet users running the system may want to screen the data sections to ensure that the Internet is being used appropriately and / or may be to ensure that no malicious code (such as viruses) is inadvertently being copied on to computers running the method. Further, using un-encrypted data does not deteriorate performance of the system by an unnecessary exchange of session keys with the result that data transfer is likely to be quicker and more efficient than methods using encryption.

Conveniently the method comprises allowing a client with a particular access level to access any datasets at that access level or below that access level. Therefore, if a client has access to datasets at the highest access level they would be able to access all datasets held on the computer system.

The method may be applicable to any computer network that contains data which it is desired to restrict access. Particular examples where it may be applicable include military, financial, health care, etc.

According to a second aspect of the invention there is provided a computer system having a store for holding data, the data being divided into a number of datasets or sections, each dataset/section having

associated with it an access level, and access determining means adapted to determine whether a client can access data at a particular access level.

Preferably the data store is held on a first computer and the access determining means is held on a second computer remote from the first. This is advantageous because it increases the security of the data held in the data store. If the access determining means and the data store are provided on the same computer it is possible that security loop holes exploited in software running on that computer may allow the access determining means to be by-passed.

Conveniently the computer system allows access to the data via a third computer which is connected to the second computer and most preferably there is no link between the first and third computers. Again this structure increases the security of the system since there is no physical link provided which allows the second computer to be by-passed.

The third computer may be provided with an input means which allows a client using the third computer to input their identity. The input means may be adapted to communicate the identity to the access determining means allowing, in use, the access determining means to determine whether that particular client can access data held on the data store.

An identification verification means may be provided and is preferably provided in association with the access determining means. The identification verification means may be adapted, in use, to verify the identity of a client using the system. The access determining means is preferably adapted to allow access to the data only once the identity of the client has been verified.

The identification verification means may be further adapted to ascertain the level of access granted to that particular client. The identification verification means may be adapted to pass level of access granted to the client to the access determining means. The access determining means may be adapted to allow the client access only to data sections which that client has clearance to access.

According to another aspect, the invention comprises a network access controller comprising a comparator which is adapted to compare a label representative of a dataset and a label representative of a user, and to determine from the comparison whether the user is authorised to have access to the dataset, the comparator being adapted to communicate with access control means adapted to allow or deny a user access to the dataset dependent upon the communication from the comparator.

Preferably, the comparator is adapted to compare a numerical value associated with the dataset label with a numerical value associated with the user. Preferably, the numerical values are binary values. Preferably, the comparator uses one or more simple binary logic operations, such as "or", "and", "nand", "nor", to make the comparison.

Preferably, the network access controller has an access control directory having a concordance between user identities and user labels. This may comprise a region of memory. There may also be provided in the comparator (or provided external of the comparator, for example at a database server), a registry of concordance between dataset identities and dataset labels.

The network access controller may comprise a computer or server. The computer may look up a user label and a dataset label and perform the comparison to determine whether access is to be denied or granted.

The network access controller may be adapted to be provided in a separate server from that which contains the database of datasets. The network access controller may be provided in a separate server from that which the user uses to access the database.

According to another aspect the invention comprises a method of controlling network access to a database held on a database server and having a plurality of datasets, the method comprising allocating each potentially accessible dataset - a dataset label, allocating a user a user label, and comprising the dataset label and user label to determine whether the user can access the dataset.

The method preferably comprises providing an access controller which controls access to the database, and providing the user labels in the access controller. Each allowable user may have a label associated with them, but a "user" could be an anonymous user that otherwise unidentified users may be able to use. The system may allocate unidentifiable users as the "anonymous user" or they may have to sign it to the access controller using an anonymous user address/code. The user labels are preferably hierarchal, with higher security clearance user labels dominating lower level security user labels and providing access to datasets of equal or lower security level or value. Preferably the method comprises providing an access control server, and a database server. The method may comprise providing the access control server and running the access control software on that server, and not the database server.

Preferably the method comprises unencrypted transfer of data from datasets for which access is granted to a user.

Preferably the method comprises running checking/blocking software on a user/browser server to screen incoming unencrypted data to block unwanted data content.

Preferably the method comprises running the access control software as a firewall to a database server. Alternatively, it may be run on a firewall of an access control server separate to the database server.

Preferably, the method comprises having a hierarchal structure to the dataset labels. This means that some datasets may be considered as sub-sets of higher order datasets, so access clearance for a higher level dataset may provide access clearance to lower level datasets as well.

Preferably, the method allocates a numerical value to the user label and the dataset label. Preferably, the values are compared to determine if access is granted or denied.

The user and/or dataset labels may have a human-readable part (e.g. a word or initials indicative of a word so that a human reader can tell what it represents without special technical machine-language knowledge). They may also have a numerical part, which may be the part the computer operates on to perform the user label/dataset label comparison.

There may be a plurality of human intelligible parts to a user label and/or dataset label (e.g. words or initials). There may be a plurality of numerical parts to a user label and/or dataset label. The numerical parts and the user parts may have a one to one correspondence.

According to another aspect the invention comprises use of any method or apparatus according to another aspect of the invention to reduce the time and/or computer memory required to manage and maintain a user-dataset security clearance/access enabling or denying concordance in a computer.

According to another aspect the invention comprises a network having a network access controller in accordance with another aspect of the invention, preferably operating in accordance with a method according to an aspect of the invention.

According to another aspect the invention comprises a software carrier carrying access control software which when operational on a computer or network either provides the apparatus or network of any other aspect of the invention, or operates the computer or network according to a method of any other aspect of the invention.

According to another aspect the invention comprises software which when running is capable of providing the apparatus or method of any aspect of the invention.

According to another aspect, the invention comprises a network comprising a user-server communicatable with, an access controller; and a potentially accessible database comprising a plurality of datasets, each of which has an associated dataset label; and the arrangement being such that in use the identity of a user is communicated to the access controller, and the access controller has a user label database of allowable user identities and user labels, each user having an allocated user label associated with them in the user label database, and a dataset label database, allocating a dataset label to each dataset potentially accessible via the access

controller, the controller being adapted to take a user identification and correlate it with a user label, take the user request for access to a specified identified dataset and determine the dataset label for the identified dataset, and compare the user label and dataset label to determine whether access is allowed or denied, data from an accessible dataset being communicated to the user server.

The network may have the user browser, communicatable with the access controller, as part of the network access controller, but it will typically be on a separate server. Preferably, the access controller and the potentially accessible database are on different physical servers, preferably at different physical locations. The physical locations may be geographically spaced out, preferably by tens or hundreds of metres, or by kilometres, or by tens, hundreds, thousands, tens of thousands of kilometres. Preferably, the access controller is provided in a secure site (physically secure site). The database of datasets may be provided on a database server, which may be a web server. The access controller is preferably provided on another, different, server to that which has the database. The access controller software preferably does not run on the database server operating software.

There may be an anonymous client present on a server which presents to the access control server an allowable identify thereby to allow a user with no known identity (to the access control server) to communicate with the access control server via the anonymous client function. The anonymous client may run on the access control server itself, or on a separate server. The unknown user may have their identity known to the anonymous client function (but not be recognised as an allowable user by the access control function). The anonymous client may be given only low (or the lowest) security value user label at the access control server.

According to another aspect, the invention comprises a network having a data-set-containing database provided at a first physical site, and a network access controller, the network access controller having telecommunication means adapted to communicate with the outside world and means communicating it with the database (preferably telecommunication means), the network access controller being provided outside of the database server.

Preferably, the network access controller does not run on the operating software of the database server.

Preferably, the network access controller is at, near, or on, the same physical site as the database server. Preferably, the arrangement is such that communication with the database can only be achieved from the outside world via the network access controller. The network access controller may be in a secure location within the first site, or near the first site (e.g. on the same property). The site may have a secure boundary, at least for the access controller. Preferably, the network has a user browser server, which is preferably provided at a second site, physically/geographically remote from the first site.

By having the network access controller on a different server than that which has the database, it is possible to have a higher level of security regarding the network access controller, and to avoid possible bypasses of the security operation required to gain access to the database occurring by bypassing an access control function running on the same server as the database, on the same operating software platform.

According to another aspect, a network access controller is provided which is adapted to allow unencrypted access to a database after an appropriate challenge/response routine has been passed by the user, the network access controller determining those parts of the database that are permissibly accessible by the particular user from a comparison of characteristics representative of the user and characteristics representative of the part of the database for which access is requested.

The controller preferably has a user identification to user label database or concordance register. The controller is preferably adapted to compare a user label with a dataset label and determine if the security value associated with the user label equals or outranks that of the dataset label.

Preferably, the network access controller is used in conjunction with an Internet network. The network may comprise a network on the worldwide web. The database may comprise one or more web pages, and the parts of the database may comprise different web pages.

Preferably, the network comprises a user browser/server. The user browser/server may be adapted to run a screening programme to check incoming unencrypted data from the accessed database to determine that it does not contain objectionable material. The objectionable material may comprise unwanted harmful software, such as viruses. The objectionable material may comprise non-allowed subject-matter detected by an appropriate subject-matter search programme.

According to another aspect, the invention comprises a network access controller having a user identification database which correlates a respective user label with each allowable user identification, the user labels having a hierarchy structure such that user labels higher up the

hierarchal structure give clearance for not only their own level of clearance, but also lower levels of clearance equivalent to lower hierarchal labels.

Preferably, the user identification database has only one user label corresponding to each user identification.

Preferably, the user identification database is adapted to have the user labels updated by an authorised person such that it is possible to delete a user identification in the user identification database (or modify or delete the label equivalent to the user identification) so as to deny a user access, or modify the level of access that they are allowed (up or down). Modification of the user label mapping to their user identification modifies the access available to a user.

According to another aspect, the invention comprises a database server or carrier having a plurality of datasets, each of which has a an associated dataset label, the dataset labels having a hierarchal structure with higher order labels requiring a higher level of security clearance before their dataset can be released than lower dataset labels.

Preferably, each database label has a security value and modification of the security value of the dataset labels modifies the security value of that label. Modification of a security label of a higher order hierarchal dataset label may modify the security value of data labels that are dominated by it. For example, if there were ten levels of dataset security value labels and the security value of level six (or a certain level) was reduced to that of level three (or a lower value), this may in certain configurations mean that the security values of levels five and four (intermediate values) were also reduced to that of level three (lower value). This may be achieved by

a single entry operation for each dataset, or a single entry operation for the entire database.

Each label (user label or dataset label) may have a plurality of different components. Each component may be allocated a numerical value. The numerical values of each of the components of a label may determine its overall security value. The numerical values of different components of the user label may be compared with the numerical values of different components of the dataset label to determine whether access is denied or granted. The comparison may be a binary operation. There may be the same number of components to a user label as to the dataset labels, or there may be a different number of components.

According to another aspect, the invention comprises a way of improving the security of a database in accordance with any of the earlier aspects of the invention.

Another aspect of the invention comprises a way of reducing the time taken to alter the security clearance of a user, for example by using any of the earlier aspects of the invention.

Another way of looking at the invention is as a method of reducing the time taken to alter the security clearance of a plurality of datasets in a database.

A further way of looking at the invention is as a way of reducing the computer memory required to compare a user identification with a dataset security clearance to determine if access is to be denied or allowed to the requested dataset, for example by using any of the earlier aspects of the invention.

The reduction in memory required may be in comparison with that required to have a user identification - dataset look up table with each dataset being mapped directly to permissible users.

A further way of looking at the invention is as a way of reducing the time and/or computer memory required to add additional users to a list of allowable users (or to delete users, or modify the security clearance of the existing users).

Another way of looking at the invention is a way of reducing the bandwidth requirement for transmission of access-controlled data to achieve a certain data rate; and/or a method of measuring the speed of transmission of access-controlled data with a given bandwidth; and/or a way of transmitting access-controlled files using lower specification computer/telecommunications equipment (compared with the transmission of encrypted data at the same data rate).

It will be appreciated that various aspects of the invention are described in relation to either software per se, a carrier carrying software, a method, apparatus (e.g. for use with a network), or a network itself. Each of the concepts of the statements of invention can be applicable to each of the species of claim type mentioned, and specific protection for each of the species in relation to each of the concepts is required.

There now follows, by way of example only, a description of the invention with reference to the accompanying drawings of which:

Figure 1 shows a block diagram of a computer network running the security arrangement;

Figure 2 shows a block diagram showing the access process for a client to access data held on the computer system;

Figure 3 shows a flow diagram of the operation of the computer network;

Figure 4 shows the Internet prior art way of mapping user identities to each potentially accessible dataset;

Figure 5 shows the present user identification to user label, and dataset identification to dataset label, mapping, and the user label to dataset label comparison; and

Figure 6 schematically shows the comparison between a user label and a dataset label.

The computer network shown in Figure 1 comprises a computer system, in this case a web server 2, containing datasets (in this case web pages 4) to which clients may which to have access. This web server 2 is connected via any known network link to a further computer system 6 running a proxy server 8 which has access to an access control list 10. To gain access to the web server 2 communications must pass through the proxy server 8.

A computer 12 can be connected to the proxy server 8 via any known communications link 14. On the computer 12 there are running at least two separate processes: some network access software (in this case a web browser) 16, and some client software 18 which tailors communications

for the proxy server 8. The client software 18 has access to a certificate 20 (an X.509 certificate) held on the computer 12.

As will be noticed from the preceding paragraph it is necessary to have the necessary client software 18 and certificate 20 in order to access the web server 2. However, in some circumstances, as will be discussed hereinafter, access may be provided for a computer 22 running the necessary access software 24 (in this case a web browser). In order to achieve this the necessary client software 26 and certificate 28 are provided on the computer system 6 running the proxy server. By connecting through a connection 30 it is possible for the computer 22 to access the web server 2.

Each piece of information held on the computer system 2 has a security level (or dataset label) associated with it. In the case of a web server a security level is assigned to each web page. To access any particular page the client must have an appropriate access level (or user label) assigned to their certificate (the certificate being used to identify that a particular client is indeed who they claim to be).

In one embodiment there exists security levels in order of restriction: unclassified, restricted, secret. A client having permission to access secret data can access any of the data, whereas a client having permission to access only unclassified data can only see data at this level. Each of the pages held on the web server 2, 4 is assigned, using an HTML meta tag, a security level (i.e. unclassified, restricted, secret) and only people having appropriate clearance will be provided with access to that page.

The access level of a particular client is determined by the proxy server 8 in conjunction with the access control list 10. Once the identity of a

client has been confirmed, as described hereinafter, the proxy server 8 controls which pages held on the web server 2 can be accessed by that particular client. Because all communication must pass through the proxy server 8 it is more secure than systems which provide access control on the same computer system that is running the web server 2. For example hackers may be able to exploit loop holes in the computer system as a whole, e.g. the operating platform software, to access data held on the web pages and thus by-pass the access control. If the operating software of the database server is well-known, e.g. NT or another widely-available commercial software, there may be a lot of people who know a lot about the software structure and who might know loopholes.

The X.509 certificate will generally hold a distinguished name which will probably show that the client is a member of a country, state (e.g. Illinois, or Warwickshire), location (e.g. address), organisation, organisational unit, common name. Each of these elements, and combinations of them, may be a means of identifying groups of people. not all elements of a distinguished name in the certificate need to be completed, for example a distinguished name may be:-

Country = GB,
Organisation = The Zoo,
Organisational Unit = Elephants,
Common Name = Mark.

In this distinguished name, Mark is a member of the following groups:

People from Great Britain.
People from Great Britain who work for 'The Zoo'.

People from Great Britain who work for 'The Zoo' in the Elephants department.

People from Great Britain who work for 'The Zoo' in the Elephants department and are called Mark.

The State and Location elements have not been completed.

Now that the server knows which groups Mark belongs to, it can check the access control list to see if there are any user label entries that match Mark's credentials. There may be any number of entries that match, and each entry will have a user security label associated with it. Each element of the distinguished name may map to a user label (or a corresponding element of a user label). In a user label library or register there does not necessarily have to be a user label for each element of the distinguished name, but there may well be. The Web page itself will also have a dataset security label associated with it. If any one of the client's labels is of an equal or greater security value than the Web page label, then Mark should be allowed access to it. If not, or if there are no matching entries, then clearly he should be denied access.

The invention assumes that there is already some mechanism for requesting and issuing X.509 certificates, and that this is a trusted process. The public certificate of the issuing Certification Authority is in the example present on the same computer as the proxy Server 8, and the public certificate and associated private key of the client is in the example present on the same computer as the client software 18.

The client's web browser must be configured in such a way that it points to the IP address and port number of the client proxy / client software 18 and all web page requests go via this proxy. The client proxy 18 must be

configured so that it points to the proxy server 8, and the proxy server 8 must be configured so that it points to the Web server 2.

As shown in Figure 3, as the client issues a web page request 50 from the web browser, the client software 18 will convey 52 this, unaltered, to the proxy server 8 which will convey 54 it, unaltered, to the web server 2. The web server 2 will generate a http response 56 after accessing the web pages 4. Upon receipt of the Web server's response, and assuming the requested page exists, the proxy server 8 will generate a string of random data and pass this, along with a request for the client's certificate 58 to the client software 18. The client software 18 will then sign the random data using it's private key, and pass the signed data and it's X.509 certificate (as stored in the client certificate store 62) back to the proxy server 8, as shown at 60. The proxy server 8 will then perform a number of checks as outlined in box 64. It will take the public key from the certificate of the issuer of the client certificate, and use this to verify that the client certificate has been correctly signed by the issuer 66. It will then check that the time period of the client certificate has not expired 68. Next, it will take the public key from the client certificate and verify that the random data has been signed correctly 70 and that the random data is the same data that the proxy server 8 issued 72. It then compares the X.509 distinguished name within the client certificate against entries in the Access Control List 74. Assuming all of the above checks have passed successfully, the proxy server 8 will compare the security label associated with the client entry in the Access Control List with that stored in the HTML source code of the requested Web Page. If the client's security label dominates 76 that of the Web page then the Web server's original response is conveyed (as shown at 78), unaltered, back to the client software 18 (as shown at 80) and then to the web browser 16 where it is displayed 82. If any of these checks fail at any time, and access

denied web page is returned, stating the reason for the denial. These denials are shown by the boxes 84 to 94 in Figure 3.

The possible reasons for the denial include: an invalid certificate response 84, 86, 88, an incorrect signed data response 90, no matching record found in the access control list 92, or there is insufficient security clearance 94. A message containing the reason is passed back via the client software and displayed on the web browser.

The access control list is held in a database with a front end that prevents any alterations being made to the design of the database, and may take the form outlined below.

Country	Organisation	Organisational Unit	Common Name	Security Label	Security Marking
GB				[3-5]	Medium
GB	'The Zoo'			[2-5]	Medium-High
US				[5-5]	Low
US	WWF	Zoo Research		[3-5]	Medium
US	WWF	Zoo Research	Alvin	[1-5]	High

As shown in Figure 1 two paths of access to the proxy server may be provided (via the client software 18 and via the link 30 by-passing the client software 18). Access via the link 30 may be used to allow people to make "anonymous" access to the system or for people who do not have the necessary client software 18 on their computer 22. Of course, it will be realised that if the necessary client software 18 is not running that it will not be possible to verify the identity of the client and that therefore the security method described herein will not be applicable. In such circumstances it would generally be appropriate for clients accessing the proxy server 18 without the client software 18 to be given the minimum level of access. For instance in the example given above it may be applicable to give such a client only access to unclassified web pages (and

thus prevent them from accessing restricted or secret web pages). Such a scheme would be realised by providing an entry in the access control list assigning the appropriate security marking someone without a certificate or who is accessing the proxy server 8 anonymously.

As well as the client software 18 and the web browser 16 it is necessary to run a client software configuration program on the computer 12. This program configures the client software 18 and provides functions such as allowing the IP address and port number of the proxy server 8 to be provided. It should be noted that as shown in Figure 1 two paths of access to the proxy server may be provided (via the client software 18 and via the anonymous link 30 by-passing the client software 18). If a client accesses the access controller anonymously, with no identification certificate, their browser will send requests for web pages through the anonymous client 26. It may be desirable to have a separate address for different proxy servers, but in the present embodiment the configuration programme has only one.

In addition to the proxy server 8 and the access control list 10 a configuration program must be run on the computer system 6 which allows the IP address and port number of the web server 2 to be stored. The configuration program also allows a default security environment to be set. The default security environment is the security level assigned to a web page if no label is present. This may be the highest level of security (so that only the highest security users can see it).

Also required on the server side (i.e. running on the computer system 6 or on the web server 2) is required a file labeller which inserts meta-tags of the correct format on to the web pages. The file labeller can be provided

with utilities which may allow any number of pages to be labelled at once which provided convenience for operators of the system.

As explained hereinbefore a more senior access level (access to secret data) will give access to less senior access levels (but not visa versa). This is based on the domination theory outlined in mathematical graph theory and may be implemented using a Unified Labelling Scheme ULS wherein a code is assigned to each access level. The codes may then be compared using simple mathematical operations such as NOT and AND to determine whether or not a user is entitled to access a particular access level.

The data from the web pages is transmitted over telecommunication lines/e.m. telecommunication lines in compressed format (unencrypted data compressed). It may be compressed by the web server. If the access control server is close the web server, this may compress the data (or some other computer may). The data received by the user's server is decompressed before it is displayed for viewing (and/or storage by the user). Alternatively, the data may be stored compressed at the web server.

A comparison between the structure of a prior art security method (SSL) and of the method of the current invention is shown in Figures 4 and 5. As can been seen in Figure 4 each dataset 100 has to contain a list of all users 102 that can access that piece of data. There must therefore effectively be a virtual connection 104 between each piece of data and a user if that user is allowed access. Not all the possible links have been shown in Figure 4 for simplicity.

As can be seen from Figure 5 the structure according to the present invention is simpler. Some users 106 are provided with respective user labels 108 and each dataset 110 is provided with a dataset label 112. Once an access to a particular dataset 110 has been requested by a user 106 a comparison process 114 compares the user label 108 with the dataset label 112 to determine whether or not access can be allowed.

It is not necessary for every user to be given an individual user label in the permissions table/library or register of user labels. Their distinguished name may itself provide clearance to a predetermined level (e.g. restricted, or unclassified), with no user-specific clearance being specified. The X.509 Certificate is user specific. The permissions table does not have to be whole groups or sets of users can be given one clearance.

Figure 6 shows one embodiment of the comparison process 114, wherein the user label 108 comprises a number of sub levels (U1, U2, U3, U4). The dataset label 110 also comprises a number of sub levels (D1, D2, D3, D4). However, the skilled person will appreciate that there could be any number of sub levels provided in the labels 108, 110 and that the number of sub levels within each label do not need to be equal. Each sub level within a label 108, 110 is assigned a numerical value (which may be binary, hexadecimal, or any other number base). The numerical value in compared using standard mathematical operations such as AND and OR and the result of this comparison is used to determine whether of not the user label 108 has sufficient authority to gain access to the data having the dataset label 110.

In one embodiment the dataset label 110 comprises two sub levels and these sub levels interact to provide the overall security level. In this

embodiment a first sub level of the dataset label contains the levels as given as an example above: unclassified, restricted, secret. The second sub level can contain any other identifier, for example apple, pear, etc. It is the combination of these two sub levels which gives the overall security level. For instance a combination of secret.apple may well have a higher security level than secret.

It will be appreciated that two significant aspects of one invention is the labelling of the client and the web page. The comparison of these two quantities forms the basis of the access control decision, and provide authenticated web access control. The technique and handware works independently of certification authorities and directory servers, and can be utilised by any web browser and web server without altering the functionality of those entities. Control of the network access controller can lie entirely in the hands of a private company or person who can control the contents of the user labels and dataset labels, and the hierarchal control database themselves. This system also provides scalability in its use of grouping users by elements of distinguished name (user labels) and mapping this to a particular security rating (dataset label). Groups of clients can have their access rights determined by the elements of the distinguished name in their user label. The X.509 Certificate, or other user-identification certificate, could form the basis of some of the sub-label regions within the user label for each user.

In the specific example given there are four server-side applications (server proxy, server proxy configuration, permissions programme, and file labeller) and two client-side applications (client proxy and client proxy configuration programme).

The file labeller may allow multiple selections of web pages (or other datasets) so that a security administrator can easily label many pages at a time.

A permissions programme maps elements of distinguished names to security labels and may be a table within an access database, with a front end that prevents any alterations.

The server proxy configuration writes information to the system registry used by the access control server. It also sets the default security environment controlling what happens if a requested web page does not contain its own security label.

The access control server is in the example given of proxy, which passes web page requests onto the web server and verifies using public/private keys that the request from the client's server has been signed correctly. If a client is denied access to a page, the access control server may inform the client of the reason why.

The client configuration proxy on the client's computer stores the Internet protocol (IP) address and port number of the access control server to which the client server connects, and the IP address and port number of the www proxy, which will allow the client to use the Internet in the normal fashion, by-passing the access control server. It may also allow the client to specify which particular certificate would be used for a particular attempt to access a dataset via the access control server.

The client proxy is a proxy on the client's server that receives a web page request from the client web browser and passes it to the access control server or the www proxy. If it has been sent to the access control server

it will receive a request for the X.509 Certificate and some random data in return. It will then sign the random data with its private key and send the data and the Certificate back to the access control server.

In practice, the owner of a database may have the database server and the access control server under their control, possibly on their property/in their buildings. They would keep and maintain the user label database and the dataset label database. A client/user would have the client server (for example Internet browser), and would have the software to run the client proxy and client configuration proxy. This software may be provided to them, for example by the database owner. It may be provided on a machine-readable data carrier (e.g. magnetic or optical disc, a tape, EPROM/ROM etc.) or it may be provided electronically (e.g. via a telecommunication link as an electrical signal or an e.m. signal).

It will be appreciated that any aspect of the present invention can be used in conjunction with any other aspect, and that the preferable features of any aspect may also be applicable to the other aspects of the invention.

The authenticat web access control system discussed is far easier to maintain and update. A maintenance manager has in the prior art website access control system to alter the allowable access identities on each web page to remove or add an allowable user. This can be very time-consuming if there are hundreds or thousands of web pages. In the new system, they simply add a new user label, or delete an existing user label from the directory of user labels (or break the correlation between identified user and their associated specific user label).

Similarly, if an entire category of web pages were to have their security access level changed (for example because a secret project had become

public/was to be made public), the maintenance manager can change the labels for those web pages to give them a lower security value. The manager may be able to do this globally in the dataset label register by, for example, putting all dataset labels with "orange" in them to the lowest, (e.g. unclassified) level if "project orange" was now public. This may be achieved by the hierarchal nature of the dataset labels. The manager may be able to enter an "orange label element to low security value" control command which may search the database labels and alter the security value of each label with "orange" in it to a low value, or alter that "orange" component of the security label to a low value.

The benefits of the present invention are best brought out in large systems with many users and/or many potentially accessible datasets. There may be of the order of hundreds or thousands of permissible users, or more. There may be of the order of thousands, tens of thousands or hundreds of thousands (or more) of datasets or web pages potentially accessible. There might be more than one secure web server (database servers) on the network. The access control server may have different addresses for different web servers and know which one to address for a request for a particular dataset (web page).

CLAIMS

1. A method of securing data held on a computer network comprising labelling datasets with an access dataset labels, determining the access level to which a user wishing to access a dataset is allowed to access by allocating users a user label and determining in the user label the level of access to be granted, and determining the user's identity and comparing the appropriate user label with the dataset label and allowing access only to datasets which have an dataset label access levels equal to or lower than the user label access level.

2. A method according to claim 1 which comprises a method of controlling access to data held on the Internet.

3. A method according to claim 2 which comprises a method of controlling access to web pages on the worldwide web.

4. A method according to claim 2 or claim 3 comprising providing the web page access levels, or dataset labels, as meta tags within the HTML code of a particular web page.

5. A method according to any preceding claim in which a user server and access controller server perform a challenge-response exchange before allowing access to those datasets for which the user is cleared for access, the access when permitted being unencrypted.

6. A method according to claim 5 in which the user server has a public and private key and signs a challenge from the access control server with its private key in returning the response to the access control server.

7. A method according to claim 5 or claim 6 in which the access control server generates random data as part of its challenge and checks that the response from the user server has properly transcribed the random data with the correct private key.

8. A method according to any one of claims 5 to 7 in which the user server runs data checking software to prevent communication of unwanted data.

9. A method according to any preceding claim in which there are a plurality of user labels with a hierarchal structure, labels in the user label hierarchy providing access to datasets which require security to their level and below.

10. A method according to any preceding claim in which the dataset labels have a hierarchal structure.

11. A method according to any preceding claim in which the user labels are allocated a numerical value and the dataset labels are allocated a numerical value and the numerical values are compared to determine whether access is denied or granted.

12. A method according to any preceding claim in which the dataset is provided on a database server and user identification and associated user label allocation and user label - dataset label comparison is performed on a separate server.

13. A method according to any preceding claim comprising using specific access-control software for determining access to datasets in database and also using standard network access software provided for accessing the network.

14. A method according to claim 13 comprising using a web browser and a web server.

15. A method according to any preceding claim comprising providing the database on a database server and access control software on a separate access controller server.

16. A method according to claim 15 which comprises providing user access request software on a user server, separate from the database and access control servers.

17. A method according to claim 13 or any claim dependent directly or indirectly from claim 13 in which the specific software provides proxy servers which communicate with the standard network access software.

18. A method according to claim 17 comprising having proxy server software on a web browser.

19. A method according to claim 17 or claim 18 comprising running proxy access controller software on either the server that has the datasets, or on a different server.

20. A method according to claim 19 in which web pages are stored on a web server and the proxy access control software is run on a different server.

21. A method according to any preceding claim in which the dataset labels have a hierarchal structure.

22. A method according to any preceding claim in which the user labels have a numerical value and the dataset labels have a numerical value and a comparison of the numerical values of a user label and a dataset label determines whether access is granted or denied.

23. A method according to claim 22 in which the comparison is to see whether the user label numerical value is greater than, less than, or equal to the dataset values.

24. A method according to claim 22 or claim 23 in which the user label and/or dataset label have different sections each with a numerical value and a comparison of the labels compares the different sections of the user label with respective corresponding sections of the dataset label.

25. A method according to claim 24 in which only if all section comparisons result in section clearance is access to the dataset provided.

26. A method according to any preceding claim in which the data transmitted to a user from the dataset is compressed for transmission.

27. A method according to any preceding claim in which there are a plurality of dataset servers on the network and an access controller directs

enquiries for data to the appropriate dataset server after it has determined that access to the dataset requested is permitted to the user in question.

28. A computer-readable medium having a programme recorded thereon in which the programme causes, in use, a computer running the programme to execute procedure to determine whether access to a dataset is to be granted or denied by retrieving a user label correspond to a user identity, retrieving a dataset label corresponding to the dataset for which a user has requested access, and comparing the user label and dataset label to provide access to data in the datasets which have dataset label access levels equal to or lower than the access level of the user level, and to deny access to datasets which have a higher access level than the user label access level.

29. A computer-readable medium according to claim 26 and adapted to cause, in use, when run on a computer the computer to perform the method of any of claims 1 to 27.

30. A computer programme element or product adapted to cause a computer loaded with the computer programme element and running the programme to perform the method of any of claims 1 to 27.

31. A computer programme element or product according to claim 30 embodied as a computer-readable medium.

32. A network access controller, comprising a comparator, which is adapted to compare a label representative of a dataset and a label representative of a user, and to determine from the comparison whether the user is authorised to have access to the dataset, the comparator being adapted to communicate with access control means adapted to allow or

deny a user access to the dataset dependent upon the communication from the comparator.

33. A controller according to claim 32 which is adapted to compare a numerical value associated with the dataset label with a numerical value associated with the user.

34. A controller according to claim 32 or claim 33 in which the numerical values are binary values and the comparator uses one or more simple binary logic operations to make the comparison.

35. A controller according to any one of claims 32 to 34 which has an access control directory having a concordance between user identities and user labels.

36. A controller according to any one of claims 32 to 35 in which the comparator has a registry of concordance between dataset identities and dataset labels.

37. A controller according to any one of claims 32 to 36 which has an anonymous client function adapted to allow users who have no recognised identity to the controller to access a network via the controller, as the anonymous client, with an access label/level determined by the anonymous client function.

38. A method of controlling network access to a database held on a database server and having a plurality of datasets, the method comprising allocating each potentially accessible dataset a dataset label, allocating a user a user label, and comparing the dataset label and user label to determine whether the user can access the dataset.

39. A method according to Claim 38 which comprises providing an access controller which controls access to the database, and providing the user labels in the access controller.

40. A method according to claim 38 or claim 39 in which each allowable user has a label associated with them and the user labels are hierarchal, with higher security clearance user labels dominating lower level security user labels and providing access to datasets of equal or lower security level or value.

41. A method according to any one of claims 38 to 40 comprising providing an access control server, and a database server, and running access control software on the access control server, and not the database server.

42. A method according to any one of claims 38 to 41 method comprising the unencrypted transfer of data from datasets for which access is granted to a user.

43. A method according to claim 42 comprising running checking/blocking software on a user/browser server to screen incoming unencrypted data to block unwanted data content.

44. A method according to any one of claims 38 to 43 comprising running the access control software as a firewall to a database server, or on a firewall of an access control server separate to the database server.

45. A method according to any one of claims 38 to 44 comprising having a hierarchal structure to the dataset labels so that some datasets

may be considered as sub-sets of higher order datasets, with access clearance for a higher level dataset providing access clearance to lower level datasets as well.

46. The use of the method of any preceding claim to reduce the human data-input time and/or computer memory required to manage and maintain a user-dataset security clearance/access enabling or denying concordance in a computer; or to reduce the bandwidth requirement for a given data transfer rate, or to increase the speed of data transmission at a given bandwidth, or to achieve a given data rate using a lower specification computer and/or telecommunications equipment.

47. A network comprising a user-browser, an access controller, and a potentially accessible database comprising a plurality of datasets, each of which has an associated dataset label, and the arrangement being such that in use the identity of a user is communicated to the access controller, and the access controller has a user label database of allowable user identities and user labels, each user having an allocated user label associated with them in the user label database, and a dataset label database, allocating a dataset label to each dataset potentially accessible via the access controller, the controller being adapted to take a user identification and correlate it with a user label, take the user request for access to a specified identified dataset and determine the dataset label for the identified dataset, and compare the user label and dataset label to determine whether access is allowed or denied.

48. A network according to claim 47 which comprises an Internet worldwide web network, with the dataset comprises web pages.

49. A network according to claim 47 or claim 48 having its user browser communicable with the access controller, as part of the network access controller, or on a separate server.

50. A network according to any of claims 47 to 49 in which the access controller and the potentially accessible database are on different physical servers at different physical locations.

51. A network having a data-set-containing database provided at a first physical site, and a network access controller, the network access controller having telecommunication means adapted to communicate with the outside world and telecommunication means communicating it with the database, the network access controller being provided outside of the database server.

52. A network according to claim 51 in which the network access controller does not run on the operating software of the database server.

53. A network according to claim 51 or claim 52 in which the network access controller is at, near, or on, the same physical site as the database server.

54. A network access controller having a user identification database which correlates a respective user label with each allowable user identification, the user labels having a hierarchal structure such that user labels higher up the hierarchal structure give clearance for not only their own level of clearance, but also lower levels of clearance equivalent to lower hierarchal labels.

55. A network according to claim 54 in which the user identification database is adapted to have the user labels updated by an authorised person such that it is possible to delete a user identification in the user identification database (or modify or delete the label equivalent to the user identification) so as to deny a user access, or modify the level of access that they are allowed (up or down).

56. A network according to claim 54 or claim 55 in which a database server or carrier has a plurality of datasets, each of which has an associated dataset label, the dataset labels having a hierarchal structure with higher order labels requiring a higher level of security clearance before their dataset can be released than lower dataset labels.

57. A method of reducing the computer processing time and/or computer memory necessary to provide authenticated access control to datasets of a database, the method comprising: allocating datasets a dataset label, authenticating whether an apparently identified user is an authenticated user by a challenge/response protocol, or other means, having a corresponding user label for each authenticated user identity, and comparing the dataset label of a user-requested dataset with the user label to determine whether access is to be denied or granted, the dataset being transmitted unencrypted if released, the reduction in processing time and/or memory requirement being in comparison with a system in which each dataset has an associated list of allowable user identities and the computer checking the specific identity of the user against the allowable list on each requested dataset, and the dataset being transmitted encrypted if released.

58. A method of updating a computer database access control program or system, the method comprising having user labels associated with

identified users, dataset labels associated with datasets of the database, and having the user labels and/or the dataset labels have an associated security value, updating of access control being performed by one or more of:

(i) adding or deleting a user and/or user label and/or the security value of a user label;

(ii) modifying the security value of a user label;

(iii) adding or deleting a dataset and/or dataset label and/or dataset label security value;

(iv) modifying the security value of a dataset label.

59. A network access controller substantially as described herein with reference to the accompanying drawings.

60. A network substantially as described herein with reference to the accompanying drawings.

61. A method of controlling access to networked data substantially as described herein with reference to the accompanying drawings.

62. A method of reducing the human time taken to manage and maintain a user/dataset access control database substantially as described herein.

63. A software carrier carrying access control software which when operational on a computer or network either provides the apparatus or network of any preceding claim, or operates the computer or network according to the method of any preceding claim.

64. A computer product or programme element which when operating on a computer causes the computer to execute procedure to perform a method in accordance with any preceding method claim, or to comprise a network access controller or network according to any preceding process controller or network claim.

65. Software which when running is capable of providing the apparatus, network, or method of any of claims 1 to 62.

ABSTRACT

IMPROVEMENTS RELATING TO SECURITY

A method of securing data held on a computer network comprising labelling datasets with an access dataset labels, determining the access level to which a user wishing to access a dataset is allowed to access by allocating users a user label and determining in the user label the level of access to be granted, and determining the user's identity and comparing the appropriate user label with the dataset label and allowing access only to datasets which have an dataset label access levels equal to or lower than the user label access level. This method is particularly relevant to Internet applications in which the datasets comprise web pages and the method is used to determine whether or not users can access particular pages.

To be accompanied, when published, by Figure 5 of the drawings.

1/4

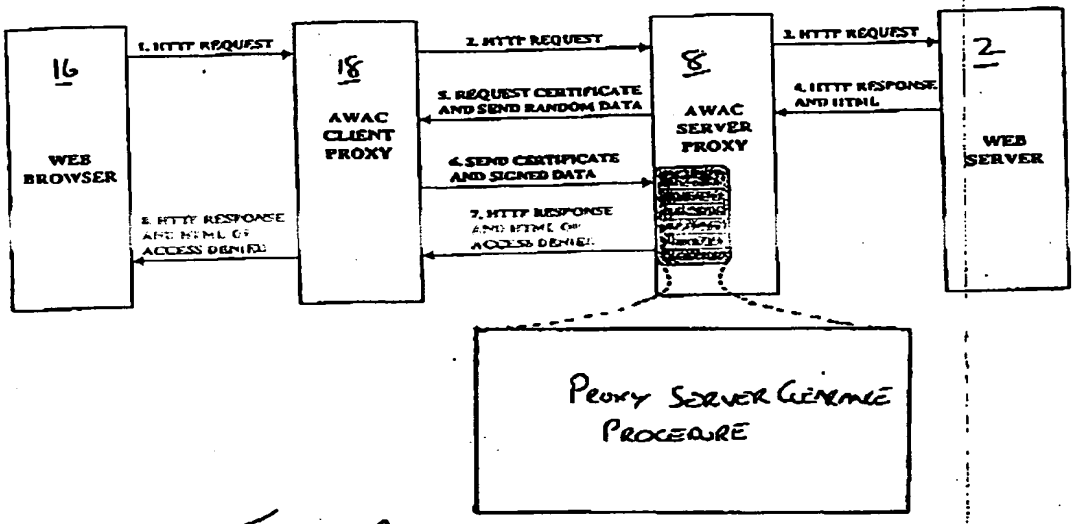

16
WEB BROWSER
1. HTTP REQUEST
8. HTTP RESPONSE AND HTML OR ACCESS DENIED
18
AWAC CLIENT PROXY
2. HTTP REQUEST
3. REQUEST CERTIFICATE AND SEND RANDOM DATA
4. SEND CERTIFICATE AND SIGNED DATA
7. HTTP RESPONSE AND HTML OR ACCESS DENIED
8
AWAC SERVER PROXY
5. HTTP REQUEST
6. HTTP RESPONSE AND HTML
2
WEB SERVER
PROXY SERVER GUARANCE PROCEDURE

FIG. 2

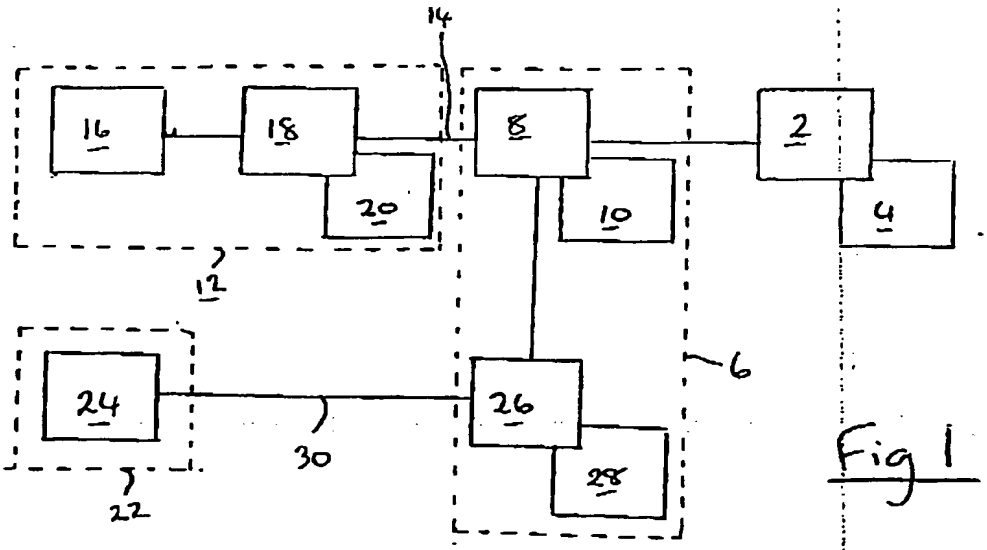

14
16
18
20
12
8
10
2
4
6
24
22
30
26
28

Fig 1

2/4

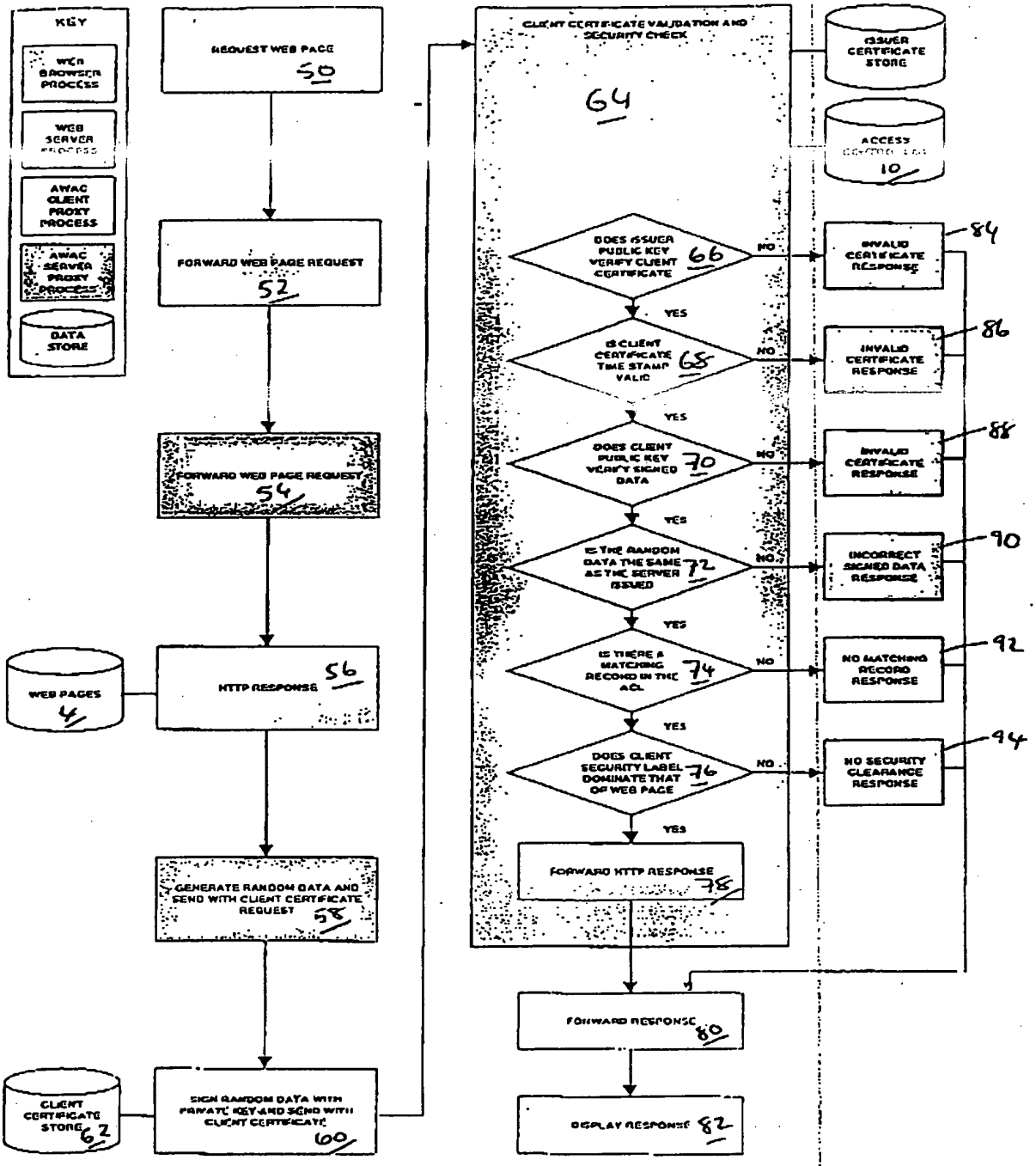
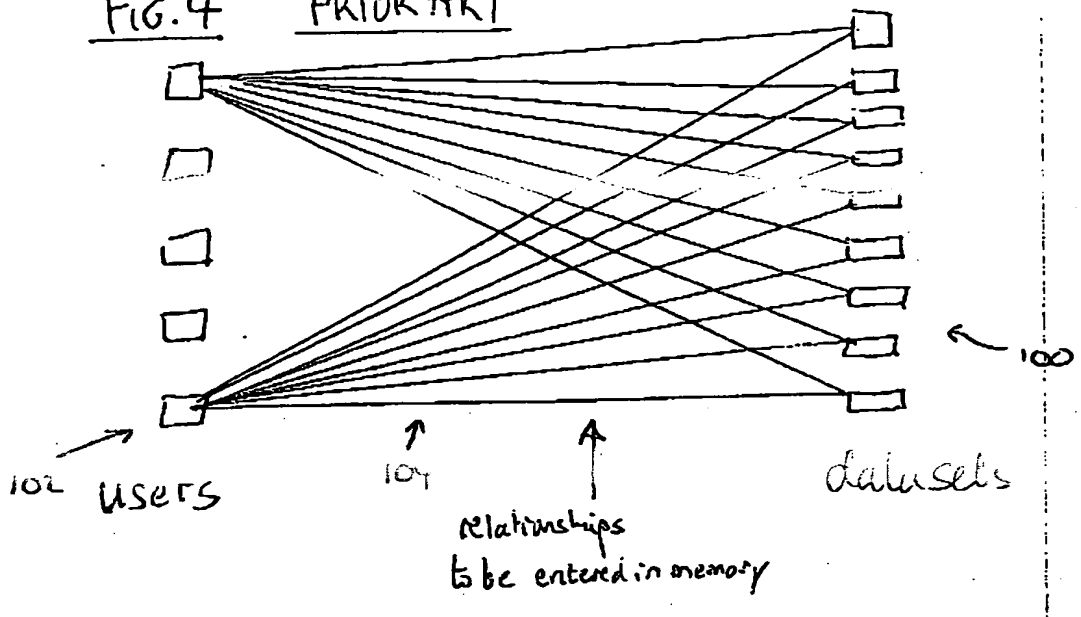

KEY
WEB BROWSER PROCESS
WEB SERVER PROCESS
AWAC CLIENT PROXY PROCESS
AWAC SERVER PROXY PROCESS
DATA STORE
REQUEST WEB PAGE 50
FORWARD WEB PAGE REQUEST 52
FORWARD WEB PAGE REQUEST 54
HTTP RESPONSE 56
WEB PAGES 4
GENERATE RANDOM DATA AND SEND WITH CLIENT CERTIFICATE REQUEST 58
SIGN RANDOM DATA WITH PRIVATE KEY AND SEND WITH CLIENT CERTIFICATE 60
CLIENT CERTIFICATE STORE 62
CLIENT CERTIFICATE VALIDATION AND SECURITY CHECK 64
ISSUER CERTIFICATE STORE
ACCESS CONTROL LIST 10
DOES ISSUER PUBLIC KEY VERIFY CLIENT CERTIFICATE 66
IS CLIENT CERTIFICATE TIME STAMP VALID 68
DOES CLIENT PUBLIC KEY VERIFY SIGNED DATA 70
IS THE RANDOM DATA THE SAME AS THE SERVER ISSUED 72
IS THERE A MATCHING RECORD IN THE ACL 74
DOES CLIENT SECURITY LABEL DOMINATE THAT OF WEB PAGE 76
FORWARD HTTP RESPONSE 78
INVALID CERTIFICATE RESPONSE 84
INVALID CERTIFICATE RESPONSE 86
INVALID CERTIFICATE RESPONSE 88
INCORRECT SIGNED DATA RESPONSE 90
NO MATCHING RECORD RESPONSE 92
NO SECURITY CLEARANCE RESPONSE 94
YES
NO
FORWARD RESPONSE 80
DISPLAY RESPONSE 82

FIG.3

FIG.4 PRIOR ART



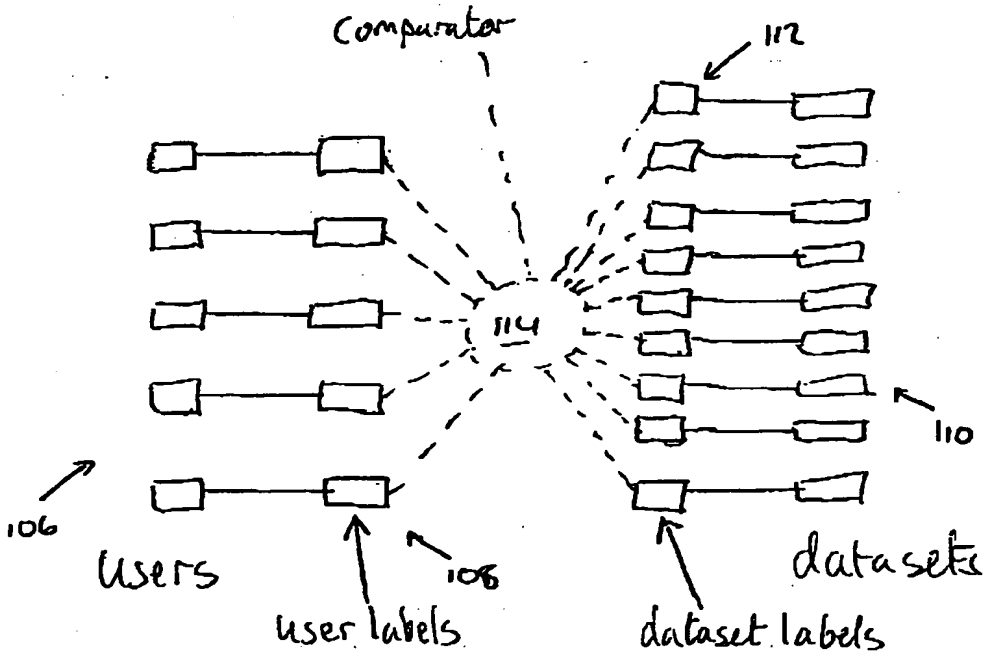


FIG.5

4/4

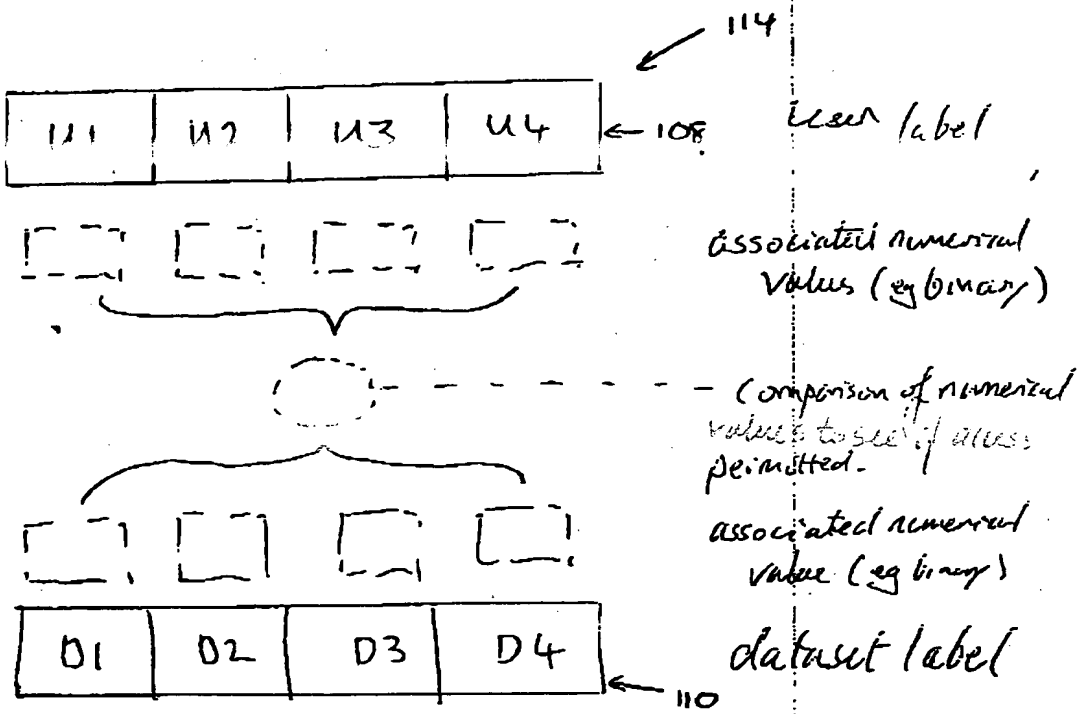

114
U1
U2
U3
U4
108
user label
associated numerical values (eg binary)
comparison of numerical values to see if access permitted.
associated numerical value (eg binary)
D1
D2
D3
D4
dataset label
110

Fig. 6

PCT/GB00/03620

Phil Treen